ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR PROVIDING HARDWARE CRYPTOGRAPHY FUNCTIONALITY TO A DATA PROCESSING SYSTEM LACKING CRYPTOGRAPHY HARDWARE

A client lacking hardware-based cryptography functionality obtains its benefits by allowing an access server (or similar server through which the client consistently transmits data transactions) which has such hardware-based cryptography functionality to act as a virtual client. A connection having packet-level encryption is employed to transmit data transaction requests, and optionally also encryption keys, digital certificates and the like assigned to the client, from the client to the server, and to transmit processed responses from the server to the client. The server performs any required security processing required for data transaction requests and responses, such as encryption/decryption or attachment or validation of digital certificates, on behalf of the client utilizing the hardware-based cryptography functionality, then forwards processed requests to recipients and returns processed responses to the client via the secure connection.